Proof of a conjecture about rotation symmetric functions *

Zhang Xiyong[1]†, Guo Hua[2], Li Yifa[1]

1.Zhengzhou Information Science and Technology Institute, PO Box 1001-745, Zhengzhou 450002, PRC

2.School of Computer Science and Engineering, Beihang University, Beijing,100083, PRC.

Abstract

Rotation symmetric Boolean functions have important applications in the design of cryptographic algorithms. We prove the conjecture about rotation symmetric Boolean functions (RSBFs) of degree 3 proposed in [1], thus the nonlinearity of such kind of functions are determined.

Keywords: *Boolean functions, Rotation-symmetric, Fourier Transform, Nonlinearity*

1 Introduction

A Boolean function $f^n(x_0, \cdots, x_{n-1})$ on n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2^n$ is the vector space of dimension n over the two element field $\mathbb{F}_2$. Rotation symmetric Boolean functions (Abbr. RSBFs) are a special kind of Boolean functions with properties that its evaluations on every cyclic inputs are the same, thus could be used as components to achieve efficient implementation in the design of a message digest algorithm in cryptography, such as MD4, MD5. These functions have attracted attentions in these years (see [2-7]). One of the main focus is the nonlinearity of these kind functions (see [6, 7]). It is known that a hashing algorithm employing degree-two RSBFs as components cannot resist the linear and differential attacks ([4]). Hence, it is necessary to use higher degree RSBFs with higher nonlinearity to protect the cryptography algorithm from differential attack. Cusick and Stănică ([1]) investigated the weight of a kind of 3-degree RSBFs and proposed a conjecture based on their numerical observations.

Conjecture 1.1 *The nonlinearity of* $F_3^n(x_0, \cdots, x_{n-1}) = \sum_{0\le i\le n-1} x_i x_{i+1(mod\ n)} x_{i+2(mod\ n)}$ *is the same as its weight.*

As claimed in [1] that if the above Conjecture could be proved, then significant progress for k-degree ($k > 3$) RSBFs might be possible. Recently Ciungu [8] proved the conjecture in the case $3|n$. In this paper, we factor F_3^n into four sub-functions, discover some recurrence relations, and thus prove the above Conjecture. The sub-functions and related recurrence are different from Cusick's[1]. The technique used in this paper may be applied for the study of RSBFs of degree $k > 3$.

We define two vectors $e_1 = (1, 0, \cdots, 0) \in \mathbb{F}_2^n$ for every $n > 1$, $e_{2^{n-1}} = (0, 0, \cdots, 0, 1) \in \mathbb{F}_2^n$, and abuse $0 = (0, \cdots, 0)$ to represent the zero vector in vector spaces $\mathbb{F}_2^n$ of every dimension for simpleness. By x^n and c^n we mean the abbr. forms of vectors $(x_0, \cdots, x_{n-1})$ and $(c_0, \cdots, c_{n-1})$ in $\mathbb{F}_2^n$. A linear function is of the form $c^n \cdot x^n$, where $\cdot$ is the vector dot product. The *weight* of a Boolean function $f^n(x^n)$ is the number of solutions $x^n \in \mathbb{F}_2^n$ such that $f^n(x^n) = 1$, denoted by $wt(f^n)$. The distance $d(f^n, g^n)$ between two Boolean functions f^n and g^n is defined to be $wt(f^n + g^n)$.

Now we list some basic definitions about Boolean functions.

*This work was supported by NSF of China with contract No. 60803154

†**Corresponding E-mail Address:** xiyong.zhang@hotmail.com

Definition 1.2 *A Boolean function $f^n(x^n)$, is called rotation symmetric if*

$$f^n(x_0, \cdots, x_{n-1}) = f^n(x_{n-1}, x_0, x_1, \cdots, x_{n-2}),\ for\ all\ (x_0, \cdots, x_{n-1}) \in \mathbb{F}_2^n.$$

Definition 1.3 *For a Boolean function $f^n(x^n)$, the Fourier transform of f^n at $c^n \in \mathbb{F}_2^n$ is defined as*

$$\widehat{f^n}(c^n) = \sum_{x^n \in \mathbb{F}_2^n} (-1)^{f^n(x^n) + c^n \cdot x^n}.$$

By the definition of Fourier transform, it is easy to see that

Lemma 1.4 *For all $(c_0, \cdots, c_{n-1}) \in \mathbb{F}_2^n$,*

$$\widehat{F_3^n}(c_0, \cdots, c_{n-1}) = \widehat{F_3^n}(c_{n-1}, c_0, \cdots, c_{n-2}).$$

Definition 1.5 *The nonlinearity N_{f^n} of a Boolean function $f^n(x^n)$, is defined as*

$$N_{f^n} = Min\ \{d(f^n(x^n), c^n \cdot x^n) | c^n \in \mathbb{F}_2^n\}.$$

By Definition 1.5, it is not difficult to deduce that for all $f^n(x^n)$,

$$\widehat{f^n}(0) = 2^n - 2 \cdot wt(f^n(x^n)).$$

Hence we can restate the above Conjecture as

$$\widehat{F_3^n}(0) = Max\{|\widehat{F_3^n}(c^n)|\ |c^n \in \mathbb{F}_2^n\}.$$

2 The proof of the Conjecture

To prove the above Conjecture, we factor F_3^n into 4 sub-functions. Let $t_n = \sum\limits_{0 \le i \le n-3} x_i x_{i+1} x_{i+2}$, and

$$\begin{aligned}
f_0^n(x_0, \cdots, x_{n-1}) &= t_n, \\
f_1^n(x_0, \cdots, x_{n-1}) &= t_n + x_0 x_1, \\
f_2^n(x_0, \cdots, x_{n-1}) &= t_n + x_{n-2} x_{n-1}, \\
f_3^n(x_0, \cdots, x_{n-1}) &= t_n + x_0 x_1 + x_{n-2} x_{n-1} + x_0 + x_{n-1}.
\end{aligned} \tag{1}$$

Then we have

$$\sum_{x_0, \cdots, x_{n-1}} (-1)^{F_3^n(x_0, \cdots, x_{n-1})} = \sum_{x_0, \cdots, x_{n-3}} \sum_{0 \le i \le 3} (-1)^{f_i^{n-2}(x_0, \cdots, x_{n-3})}.$$

Lemma 2.1 *For every $c^n = (c_0, \cdots, c_{n-1}) \in \mathbb{F}_2^n$, if $c_{n-1} = 0$, then*

$$\begin{aligned}
\widehat{f_0^n}(c^n) &= 2(\widehat{f_0^{n-2}}(c^{n-2}) + (-1)^{c_{n-2}} \cdot \widehat{f_0^{n-3}}(c^{n-3})), \\
\widehat{f_1^n}(c^n) &= 2(\widehat{f_1^{n-2}}(c^{n-2}) + (-1)^{c_{n-2}} \cdot \widehat{f_1^{n-3}}(c^{n-3})), \\
\widehat{f_2^n}(c^n) &= 2(\widehat{f_0^{n-2}}(c^{n-2}) + (-1)^{c_{n-3} + c_{n-2}} \cdot \widehat{f_2^{n-3}}(c^{n-3} + e_{2^{n-4}})), \\
\widehat{f_3^n}(c^n) &= 2(-1)^{c_{n-2}} \cdot \widehat{f_1^{n-3}}(c^{n-3} + e_1),
\end{aligned} \tag{2}$$

where $c^{n-2} \in \mathbb{F}_2^{n-2}$ and $c^{n-3} \in \mathbb{F}_2^{n-3}$ are the first $n-2$ and $n-3$ bits of $c^n \in \mathbb{F}_2^n$, and $e_1 = (1, 0, \cdots, 0), e_{2^{n-4}} = (0, \cdots, 0, 1) \in \mathbb{F}_2^{n-3}$.

Proof. We prove the first relation, proof of the other three ones are similar. Because $c_{n-1} = 0$, we have

$$
\begin{aligned}
&\widehat{f_0^n}(c^n)\\
&= \sum_{x^n:x_{n-1}=0}(-1)^{f_0^n(x^n)+c^n\cdot x^n} + \sum_{x^n:x_{n-1}=1}(-1)^{f_0^n(x^n)+c^n\cdot x^n}\\
&= \sum_{x^{n-1}}(-1)^{f_0^{n-1}(x^{n-1})+c^{n-1}\cdot x^{n-1}} + \sum_{x^{n-1}}(-1)^{f_0^{n-1}(x^{n-1})+x_{n-3}x_{n-2}+c^{n-1}\cdot x^{n-1}}\\
&= \sum_{x^{n-1}:x_{n-2}=0}(-1)^{f_0^{n-1}(x^{n-1})+c^{n-1}\cdot x^{n-1}} + \sum_{x^{n-1}:x_{n-2}=0}(-1)^{f_0^{n-1}(x^{n-1})+x_{n-3}x_{n-2}+c^{n-1}\cdot x^{n-1}}\\
&\quad + \sum_{x^{n-1}:x_{n-2}=1}(-1)^{f_0^{n-1}(x^{n-1})+c^{n-1}\cdot x^{n-1}} + \sum_{x^{n-1}:x_{n-2}=1}(-1)^{f_0^{n-1}(x^{n-1})+x_{n-3}x_{n-2}+c^{n-1}\cdot x^{n-1}}
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{x^{n-2}}(-1)^{f_0^{n-2}(x^{n-2})+c^{n-2}\cdot x^{n-2}} + \sum_{x^{n-2}}(-1)^{f_0^{n-2}(x^{n-2})+c^{n-2}\cdot x^{n-2}}\\
&\quad + \sum_{x^{n-2}}(-1)^{f_0^{n-2}(x^{n-2})+c^{n-2}\cdot x^{n-2}+x_{n-4}x_{n-3}+c_{n-2}}\\
&\quad + \sum_{x^{n-2}}(-1)^{f_0^{n-2}(x^{n-2})+c^{n-2}\cdot x^{n-2}+x_{n-4}x_{n-3}+x_{n-3}+c_{n-2}}\\
&= 2\cdot\widehat{f_0^{n-2}}(c^{n-2})\\
&\quad + \sum_{x^{n-2}:x_{n-3}=0}(-1)^{f_0^{n-2}(x^{n-2})+c^{n-2}\cdot x^{n-2}+x_{n-4}x_{n-3}+c_{n-2}}\\
&\quad + \sum_{x^{n-2}:x_{n-3}=1}(-1)^{f_0^{n-2}(x^{n-2})+c^{n-2}\cdot x^{n-2}+x_{n-4}x_{n-3}+c_{n-2}}\\
&\quad + \sum_{x^{n-2}:x_{n-3}=0}(-1)^{f_0^{n-2}(x^{n-2})+c^{n-2}\cdot x^{n-2}+x_{n-4}x_{n-3}+x_{n-3}+c_{n-2}}\\
&\quad + \sum_{x^{n-2}:x_{n-3}=1}(-1)^{f_0^{n-2}(x^{n-2})+c^{n-2}\cdot x^{n-2}+x_{n-4}x_{n-3}+x_{n-3}+c_{n-2}}\\
&= 2\cdot\widehat{f_0^{n-2}}(c^{n-2})\\
&\quad + \sum_{x^{n-3}}(-1)^{f_0^{n-3}(x^{n-3})+c^{n-3}\cdot x^{n-3}+c_{n-2}}\\
&\quad + \sum_{x^{n-3}}(-1)^{f_0^{n-3}(x^{n-3})+c^{n-3}\cdot x^{n-3}+c_{n-2}}\\
&\quad + \sum_{x^{n-3}}(-1)^{f_0^{n-3}(x^{n-3})+c^{n-3}\cdot x^{n-3}+x_{n-5}x_{n-4}+x_{n-4}+c_{n-3}+c_{n-2}}\\
&\quad + \sum_{x^{n-3}}(-1)^{f_0^{n-3}(x^{n-3})+c^{n-3}\cdot x^{n-3}+x_{n-5}x_{n-4}+x_{n-4}+c_{n-3}+c_{n-2}+1}\\
&= 2\cdot\widehat{f_0^{n-2}}(c^{n-2}) + 2\cdot(-1)^{c_{n-2}}\cdot\widehat{f_0^{n-3}}(c^{n-3})\\
&\quad + \sum_{x^{n-3}}(-1)^{f_0^{n-3}(x^{n-3})+c^{n-3}\cdot x^{n-3}+x_{n-5}x_{n-4}+x_{n-4}+c_{n-3}+c_{n-2}}\\
&\quad - \sum_{x^{n-3}}(-1)^{f_0^{n-3}(x^{n-3})+c^{n-3}\cdot x^{n-3}+x_{n-5}x_{n-4}+x_{n-4}+c_{n-3}+c_{n-2}}\\
&= 2\cdot\widehat{f_0^{n-2}}(c^{n-2}) + 2\cdot(-1)^{c_{n-2}}\cdot\widehat{f_0^{n-3}}(c^{n-3}).
\end{aligned}
$$

■

Lemma 2.2 *For every $c^n = (c_0, \cdots, c_{n-1}) \in \mathbb{F}_2^n$, if $c_{n-1} = 1$, then for $i = 0, 2$,*

$$
\begin{aligned}
\widehat{f_i^n}(c^n) &= \widehat{f_0^{n-1}}(c^{n-1}) \pm 2\cdot\widehat{f_0^{n-4}}(c^{n-4})),\\
\textit{or} \quad &= \widehat{f_0^{n-1}}(c^{n-1}) \pm 2\cdot\widehat{f_0^{n-4}}(c^{n-4}) \pm 4\cdot\widehat{f_2^{n-5}}(c^{n-5}),\\
\textit{or} \quad &= \widehat{f_0^{n-1}}(c^{n-1}) \pm 2\cdot\widehat{f_0^{n-4}}(c^{n-4}) \pm 4\cdot\widehat{f_2^{n-5}}(c^{n-5}+e_{2^{n-6}}),
\end{aligned}
\tag{3}
$$

and for $i = 1$,

$$
\begin{aligned}
\widehat{f_i^n}(c^n) &= \widehat{f_1^{n-1}}(c^{n-1}) \pm 2\cdot\widehat{f_1^{n-4}}(c^{n-4}),\\
\textit{or} \quad &= \widehat{f_1^{n-1}}(c^{n-1}) \pm 2\cdot\widehat{f_1^{n-4}}(c^{n-4}) \pm 4\cdot\widehat{f_1^{n-5}}(c^{n-5}),\\
\textit{or} \quad &= \widehat{f_1^{n-1}}(c^{n-1}) \pm 2\cdot\widehat{f_1^{n-4}}(c^{n-4}) \pm 4\cdot\widehat{f_3^{n-5}}(c^{n-5}+e_1),
\end{aligned}
\tag{4}
$$

and for $i=3$,

$$\begin{array}{rl} \widehat{f_i^n}(c^n) & = \widehat{f_1^{n-1}}(c^{n-1}+e_1) \pm 2\cdot \widehat{f_1^{n-4}}(c^{n-4}+e_1), \\ or & = \widehat{f_1^{n-1}}(c^{n-1}+e_1) \pm 2\cdot \widehat{f_1^{n-4}}(c^{n-4}+e_1) \pm 4\cdot \widehat{f_1^{n-5}}(c^{n-5}+e_1), \\ or & = \widehat{f_1^{n-1}}(c^{n-1}+e_1) \pm 2\cdot \widehat{f_1^{n-4}}(c^{n-4}+e_1) \pm 4\cdot \widehat{f_3^{n-5}}(c^{n-5}), \end{array} \tag{5}$$

where $c^{n-1}\in\mathbb{F}_2^{n-1}$, $c^{n-4}\in\mathbb{F}_2^{n-4}$, *and* $c^{n-5}\in\mathbb{F}_2^{n-5}$ *are the first* $n-1$, $n-4$ *and* $n-5$ *bits of* $c^n\in\mathbb{F}_2^n$, *and* $e_1=(1,0,\cdots,0), e_{2^{n-6}}=(0,\cdots,0,1)\in\mathbb{F}_2^{n-5}$.

Proof. We briefly prove the relations for f_0^n, f_2^n.
Because $c_{n-1}=1$, we have

$$\begin{array}{l} \widehat{f_0^n}(c^n) \\ = \sum\limits_{x^n:x_{n-1}=0}(-1)^{f_0^n(x^n)+c^n\cdot x^n} + \sum\limits_{x^n:x_{n-1}=1}(-1)^{f_0^n(x^n)+c^n\cdot x^n} \\ = \widehat{f_0^{n-1}}(c^{n-1}) + \sum\limits_{0\le j\le 7}(-1)^{g_{0,j}^{n-4}}. \end{array} \tag{6}$$

where $g_{0,j}^{n-4}(x_0,\cdots,x_{n-5})$ are functions corresponding to $f_0^n(x^n)+c^n\cdot x^n$ where $c_{n-1}=1, x_{n-1}=1, j=x_{n-4}+2x_{n-3}+4x_{n-2}$. Calculate these functions in details in Table 1.

$j:(x_{n-4},x_{n-3},x_{n-2})$	$g_{0,j}^{n-4}$
$(0,0,0)$	$f_0^{n-4}+c^{n-4}\cdot x^{n-4}+1$
$(1,0,0)$	$f_0^{n-4}+c^{n-4}\cdot x^{n-4}+x_{n-6}x_{n-5}+c_{n-4}+1$
$(0,1,0)$	$f_0^{n-4}+c^{n-4}\cdot x^{n-4}+c_{n-3}+1$
$(0,0,1)$	$f_0^{n-4}+c^{n-4}\cdot x^{n-4}+c_{n-2}+1$
$(1,1,0)$	$f_0^{n-4}+c^{n-4}\cdot x^{n-4}+x_{n-6}x_{n-5}+x_{n-5}+c_{n-4}+c_{n-3}+1$
$(1,0,1)$	$f_0^{n-4}+c^{n-4}\cdot x^{n-4}+x_{n-6}x_{n-5}+c_{n-4}+c_{n-2}+1$
$(0,1,1)$	$f_0^{n-4}+c^{n-4}\cdot x^{n-4}+c_{n-3}+c_{n-2}$
$(1,1,1)$	$f_0^{n-4}+c^{n-4}\cdot x^{n-4}+x_{n-6}x_{n-5}+x_{n-5}+c_{n-4}+c_{n-3}+c_{n-2}+1$

Table 1: $g_{0,j}^{n-4}(0\le j\le 7)$ corresponding to $f_0^n(x^n)+c^n\cdot x^n$.

By Table 1, we have

$$\begin{array}{l} \sum\limits_{0\le j\le 7}(-1)^{g_{0,j}^{n-4}} \\ = ((-1)+(-1)^{c_{n-2}+1}+(-1)^{c_{n-3}+1}+(-1)^{c_{n-3}+c_{n-2}})\cdot \widehat{f_0^{n-4}}(c^{n-4}) \\ \quad +(-1)^{c_{n-4}+1}(1+(-1)^{c_{n-2}})\cdot \widehat{f_2^{n-4}}(c^{n-4}) \\ \quad +(-1)^{c_{n-4}+c_{n-3}+1}(1+(-1)^{c_{n-2}})\cdot \widehat{f_2^{n-4}}(c^{n-4}+e_{2^{n-5}}) \\ = \begin{cases} -2(-1)^{c_{n-3}}\widehat{f_0^{n-4}}(c^{n-4}) & if\ c_{n-2}=1, \\ -2\widehat{f_0^{n-4}}(c^{n-4})-4(-1)^{c_{n-4}}\widehat{f_0^{n-5}}(c^{n-5}) & if\ c_{n-2}=0, c_{n-3}=0, \\ -2\widehat{f_0^{n-4}}(c^{n-4})-4(-1)^{c_{n-4}+c_{n-5}}\widehat{f_2^{n-5}}(c^{n-5}+e_{2^{n-6}}) & if\ c_{n-2}=0, c_{n-3}=1. \end{cases} \end{array} \tag{7}$$

So we have

$$\begin{array}{l} \widehat{f_0^n}(c^n) \\ = \begin{cases} \widehat{f_0^{n-1}}(c^{n-1})-2(-1)^{c_{n-3}}\widehat{f_0^{n-4}}(c^{n-4}) & if\ c_{n-2}=1, \\ \widehat{f_0^{n-1}}(c^{n-1})-2\widehat{f_0^{n-4}}(c^{n-4})-4(-1)^{c_{n-4}}\widehat{f_0^{n-5}}(c^{n-5}) & if\ c_{n-2}=0, c_{n-3}=0, \\ \widehat{f_0^{n-1}}(c^{n-1})-2\widehat{f_0^{n-4}}(c^{n-4})-4(-1)^{c_{n-4}+c_{n-5}}\widehat{f_2^{n-5}}(c^{n-5}+e_{2^{n-6}}) & if\ c_{n-2}=0, c_{n-3}=1. \end{cases} \end{array} \tag{8}$$

For the proof of the relation of f_2^n, we list the functions $g_{2,j}^{n-4}(0\le j\le 7)$ corresponding to $f_2^n(x^n)+c^n\cdot x^n$ in Table 2, where $c_{n-1}=1, x_{n-1}=1, j=x_{n-4}+2x_{n-3}+4x_{n-2}$.

$j : (x_{n-4}, x_{n-3}, x_{n-2})$	$g_{2,j}^{n-4}$
$(0,0,0)$	$f_0^{n-4} + c^{n-4} \cdot x^{n-4} + 1$
$(1,0,0)$	$f_0^{n-4} + c^{n-4} \cdot x^{n-4} + x_{n-6}x_{n-5} + c_{n-4} + 1$
$(0,1,0)$	$f_0^{n-4} + c^{n-4} \cdot x^{n-4} + c_{n-3} + 1$
$(0,0,1)$	$f_0^{n-4} + c^{n-4} \cdot x^{n-4} + c_{n-2}$
$(1,1,0)$	$f_0^{n-4} + c^{n-4} \cdot x^{n-4} + x_{n-6}x_{n-5} + x_{n-5} + c_{n-4} + c_{n-3} + 1$
$(1,0,1)$	$f_0^{n-4} + c^{n-4} \cdot x^{n-4} + x_{n-6}x_{n-5} + c_{n-4} + c_{n-2}$
$(0,1,1)$	$f_0^{n-4} + c^{n-4} \cdot x^{n-4} + c_{n-3} + c_{n-2} + 1$
$(1,1,1)$	$f_0^{n-4} + c^{n-4} \cdot x^{n-4} + x_{n-6}x_{n-5} + x_{n-5} + c_{n-4} + c_{n-3} + c_{n-2}$

Table 2: $g_{2,j}^{n-4}(0 \le j \le 7)$ corresponding to $f_2^n(x^n) + c^n \cdot x^n$.

Similarly

$$\begin{aligned}
&\widehat{f_2^n}(c^n) \\
&= \sum_{x^n : x_{n-1}=0} (-1)^{f_2^n(x^n)+c^n\cdot x^n} + \sum_{x^n : x_{n-1}=1} (-1)^{f_2^n(x^n)+c^n\cdot x^n} \\
&= \widehat{f_0^{n-1}}(c^{n-1}) + \sum_{0\le j\le 7} (-1)^{g_{2,j}^{n-4}},
\end{aligned} \tag{9}$$

And

$$\begin{aligned}
&\sum_{0\le j\le 7} (-1)^{g_{2,j}^{n-4}} \\
&= ((-1) + (-1)^{c_{n-2}} + (-1)^{c_{n-3}+1} + (-1)^{c_{n-3}+c_{n-2}+1}) \cdot \widehat{f_0^{n-4}}(c^{n-4}) \\
&\quad +(-1)^{c_{n-4}}((-1) + (-1)^{c_{n-2}}) \cdot \widehat{f_2^{n-4}}(c^{n-4}) \\
&\quad +(-1)^{c_{n-4}+c_{n-3}}((-1) + (-1)^{c_{n-2}}) \cdot \widehat{f_2^{n-4}}(c^{n-4} + e_{2^{n-5}}) \\
&= \begin{cases} -2(-1)^{c_{n-3}}\widehat{f_0^{n-4}}(c^{n-4}) & if\ c_{n-2} = 0, \\ -2\widehat{f_0^{n-4}}(c^{n-4}) - 4(-1)^{c_{n-4}}\widehat{f_0^{n-5}}(c^{n-5}) & if\ c_{n-2} = 1\ and\ c_{n-3} = 0, \\ -2\widehat{f_0^{n-4}}(c^{n-4}) - 4(-1)^{c_{n-4}+c_{n-5}}\widehat{f_2^{n-5}}(c^{n-5} + e_{2^{n-6}}) & if\ c_{n-2} = 1\ and\ c_{n-3} = 1. \end{cases}
\end{aligned} \tag{10}$$

By (9) and (10), the relation for f_2^n follows.
Similarly, $\widehat{f_1^n}(c^n) = \widehat{f_1^{n-1}}(c^{n-1}) + \sum_{0\le j\le 7} (-1)^{g_{1,j}^{n-4}}$, where $\sum_{0\le j\le 7} (-1)^{g_{1,j}^{n-4}}$ can be calculated as

$$\begin{aligned}
&\sum_{0\le j\le 7} (-1)^{g_{1,j}^{n-4}} \\
&= \begin{cases} -2(-1)^{c_{n-3}}\widehat{f_1^{n-4}}(c^{n-4}) & if\ c_{n-2} = 1, \\ -2\widehat{f_1^{n-4}}(c^{n-4}) - 4(-1)^{c_{n-4}}\widehat{f_1^{n-5}}(c^{n-5}) & if\ c_{n-2} = 0\ and\ c_{n-3} = 0, \\ -2\widehat{f_1^{n-4}}(c^{n-4}) - 4(-1)^{c_{n-4}+c_{n-5}}\widehat{f_3^{n-5}}(c^{n-5} + e_1) & if\ c_{n-2} = 0\ and\ c_{n-3} = 1. \end{cases}
\end{aligned} \tag{11}$$

Similarly again, $\widehat{f_3^n}(c^n) = \widehat{f_1^{n-1}}(c^{n-1} + e_1) + \sum_{0\le j\le 7} (-1)^{g_{3,j}^{n-4}}$, where $\sum_{0\le j\le 7} (-1)^{g_{3,j}^{n-4}}$ can be calculated as

$$\begin{aligned}
&\sum_{0\le j\le 7} (-1)^{g_{3,j}^{n-4}} \\
&= \begin{cases} 2(-1)^{c_{n-3}}\widehat{f_1^{n-4}}(c^{n-4} + e_1) & if\ c_{n-2} = 0, \\ 2\widehat{f_1^{n-4}}(c^{n-4} + e_1) + 4(-1)^{c_{n-4}}\widehat{f_1^{n-5}}(c^{n-5} + e_1) & if\ c_{n-2} = 1\ and\ c_{n-3} = 0, \\ 2\widehat{f_1^{n-4}}(c^{n-4} + e_1) + 4(-1)^{c_{n-4}+c_{n-5}}\widehat{f_3^{n-5}}(c^{n-5}) & if\ c_{n-2} = 1\ and\ c_{n-3} = 1. \end{cases}
\end{aligned} \tag{12}$$

■

Cusick and Stănică[1] have proved that $wt(F_3^n(x)) = 2(wt(F_3^{n-2}(x)) + wt(F_3^{n-3}(x))) + 2^{n-3}$, i.e. $\widehat{F_3^n}(0) = 2(\widehat{F_3^{n-2}}(0) + \widehat{F_3^{n-3}}(0))$ (in fact it could also be verified by Lemma 2.1 and Lemma 2.2). The following Lemma gives more relations about $\widehat{F_3^n}(0)$.

Lemma 2.3 $\widehat{F_3^n}(0)$ *satisfies the following relationships:*

$$\begin{array}{lll} \widehat{F_3^n}(0) & = \widehat{F_3^{n-1}}(0) + 2\widehat{F_3^{n-4}}(0) + 4\widehat{F_3^{n-5}}(0) & n \geq 8, \\ \widehat{F_3^{n-1}}(0) & \leq \widehat{F_3^n}(0) \leq 2\widehat{F_3^{n-1}}(0), & n \geq 7. \end{array} \tag{13}$$

Proof. For the first equation, by the recurrence relation $\widehat{F^n}(0) = 2(\widehat{F^{n-2}}(0) + \widehat{F^{n-3}}(0))$, we have for all $n \geq 8$,

$$\begin{array}{l} \widehat{F_3^n}(0) = 2(\widehat{F_3^{n-2}}(0) + \widehat{F_3^{n-3}}(0)), \\ \widehat{F_3^{n-1}}(0) = 2(\widehat{F_3^{n-3}}(0) + \widehat{F_3^{n-4}}(0)), \\ 2\widehat{F_3^{n-2}}(0) = 4(\widehat{F_3^{n-4}}(0) + \widehat{F_3^{n-5}}(0)), \end{array} \tag{14}$$

Calculating "$the\ first\ equation\ -\ the\ second\ equation\ +\ the\ third\ equation$", we obtain

$$\widehat{F_3^n}(0) = \widehat{F_3^{n-1}}(0) + 2\widehat{F_3^{n-4}}(0) + 4\widehat{F_3^{n-5}}(0).$$

$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$	$n=9$	$n=10$
6	8	20	28	56	96	168	304

Table 3: The values of $\widehat{F_3^n}(0)$.

It is obvious $\widehat{F^{n-1}}(0) \leq \widehat{F^n}(0)$ for all $n \geq 4$. For the proof of $\widehat{F^n}(0) \leq 2\widehat{F^{n-1}}(0)$, we show it by induction. From Table 3, it is true for $n < 7$. Assume it is true for all $n \leq s, n, s \geq 7$, we prove it for the case $s+1$. Since

$$\begin{array}{ll} \widehat{F_3^{s-1}}(0) & \leq 2\widehat{F_3^{s-2}}(0), (by\ assumption) \\ \widehat{F_3^{s-2}}(0) & \leq 2\widehat{F_3^{s-3}}(0), (by\ assumption) \\ \widehat{F_3^{s}}(0) & = 2(\widehat{F_3^{s-2}}(0) + \widehat{F_3^{s-3}}(0)), \\ \widehat{F_3^{s+1}}(0) & = 2(\widehat{F_3^{s-1}}(0) + \widehat{F_3^{s-2}}(0)), \end{array} \tag{15}$$

It follows from the above relationships that

$$\widehat{F_3^{s+1}}(0) \leq 2\widehat{F_3^{s}}(0).$$

■

Lemma 2.4 *Let* $c^n = (c_0, \cdots, c_{n-1}) \in \mathbb{F}_2^n$. *If* $c_1 = 1$, *then*

$$|\widehat{f_i^n}(c^n)| \leq \frac{1}{4} \cdot \widehat{F_3^{n+2}}(0), (0 \leq i \leq 3, n \geq 9).$$

Proof. We prove it by induction. Firstly with the help of computer, we verify that for all $n \in [3, 9], c^n \neq 0$, $|\widehat{f_i^n}(c^n)| < \frac{1}{4} \cdot \widehat{F_3^{n+2}}(0), (0 \leq i \leq 3)$. (For example, see Table 4 for the case $n = 6$. In this case $\widehat{F_3^{n+2}}(0) = \widehat{F_3^8}(0) = 96$, and we see that $|\widehat{f_i^6}(c^6)| < \frac{1}{4} \cdot \widehat{F_3^8}(0) = 24, (0 \leq i \leq 3)$). Assume the claim is true for all $n < s$, where $n \geq 9, s \geq 10$, we now prove it is true for s.

Since $c_1 = 1$, we have $c^n, c^{n-1}, c^{n-2}, c^{n-3}, c^{n-4}, c^{n-5}$ are all not zero vectors.

$(0, 36, 28, 28, 4)$	$(1, 4, 12, 4, 12)$	$(2, 12, 20, 4, -4)$	$(3, -4, -12, -4, 4)$
$(4, 12, -4, 20, 4)$	$(5, -4, 12, -4, -4)$	$(6, -12, 4, -4, -4)$	$(7, 4, -12, 4, 4)$
$(8, 12, 20, -4, 4)$	$(9, 12, 4, 4, 12)$	$(10, 4, -4, 4, -4)$	$(11, -12, -4, -4, 4)$
$(12, 4, -12, -12, 4)$	$(13, -12, 4, -4, -4)$	$(14, -4, 12, -4, -4)$	$(15, 12, -4, 4, 4)$
$(16, 12, 4, 20, -4)$	$(17, -4, 4, -4, -12)$	$(18, 4, 12, 12, 4)$	$(19, 4, -4, 4, -4)$
$(20, 4, 4, -4, -4)$	$(21, 4, 4, 4, 4)$	$(22, -4, -4, -12, 4)$	$(23, -4, -4, -4, -4)$
$(24, -12, -4, 4, -4)$	$(25, 4, -4, 12, -12)$	$(26, -4, -12, -4, 4)$	$(27, -4, 4, -12, -4)$
$(28, -4, -4, 12, -4)$	$(29, -4, -4, -12, 4)$	$(30, 4, 4, 4, 4)$	$(31, 4, 4, 12, -4)$
$(32, 4, 4, 12, 12)$	$(33, 4, 4, 4, 20)$	$(34, -4, -4, 4, -12)$	$(35, -4, -4, -4, 12)$
$(36, 12, 4, 4, 12)$	$(37, -4, 4, -4, 4)$	$(38, 4, 12, -4, -12)$	$(39, 4, -4, 4, 12)$
$(40, -4, -4, 12, -4)$	$(41, -4, -4, 4, 4)$	$(42, 4, 4, 4, 4)$	$(43, 4, 4, -4, -4)$
$(44, -12, -4, 4, -4)$	$(45, 4, -4, -4, -12)$	$(46, -4, -12, -4, 4)$	$(47, -4, 4, 4, -4)$
$(48, -4, -4, -12, 4)$	$(49, -4, -4, -4, 12)$	$(50, 4, 4, -4, -4)$	$(51, 4, 4, 4, 20)$
$(52, -12, -4, -4, 4)$	$(53, 4, -4, 4, -4)$	$(54, -4, -12, 4, -4)$	$(55, -4, 4, -4, -12)$
$(56, 4, 4, -12, 4)$	$(57, 4, 4, -4, 12)$	$(58, -4, -4, -4, -4)$	$(59, -4, -4, 4, -12)$
$(60, 12, 4, -4, 4)$	$(61, -4, 4, 4, -4)$	$(62, 4, 12, 4, -4)$	$(63, 4, -4, -4, 20)$

Table 4: $(c, \widehat{f_0^6}(c), \widehat{f_1^6}(c), \widehat{f_2^6}(c), \widehat{f_3^6}(c))$, where $c = (c_0, \cdots, c_5) \in \mathbb{F}_2^6$ is represented by its corresponding integer number $\sum_{0 \le i \le 5} c_i 2^i$.

If $c_{n-1} = 0$, then by Lemma 2.1 and Lemma 2.3, we have

$$\begin{aligned}
&\left|\widehat{f_0^s}(c^s)\right| \\
&= \left|2(\widehat{f_0^{s-2}}(c^{s-2}) + (-1)^{c_{n-2}} \cdot \widehat{f_0^{s-3}}(c^{s-3}))\right| \\
&\le \left|2(\widehat{f_0^{s-2}}(c^{s-2})\right| + 2\left|\widehat{f_0^{s-3}}(c^{s-3}))\right| \\
&< \tfrac{1}{4} \cdot (2(\widehat{F_3^s}(0) + \widehat{F_3^{s-1}}(0))) \\
&= \tfrac{1}{4} \cdot \widehat{F_3^{s+2}}(0).
\end{aligned} \tag{16}$$

Similarly, the case for $|\widehat{f_i^n}(c^n)| < \frac{1}{4} \cdot \widehat{F^{n+2}}(0), (i = 1, 2)$ can be proven.
For the case $i = 3$, we have

$$\begin{aligned}
\left|\widehat{f_3^s}(c^s)\right| &= \left|2(-1)^{c_{s-2}} \cdot \widehat{f_1^{s-3}}(c^{s-3} + e_1)\right| \\
&= \left|2 \cdot \widehat{f_1^{s-3}}(c^{s-3} + e_1)\right| \\
&< \tfrac{1}{4} \cdot 2\widehat{F_3^{s-1}}(0) \\
&< \tfrac{1}{4} \cdot (2\widehat{F_3^{s-1}}(0) + 2\widehat{F_3^s}(0)) \\
&= \tfrac{1}{4} \cdot \widehat{F_3^{s+2}}(0).
\end{aligned} \tag{17}$$

If $c_{n-1} = 1$, we prove the case $i = 0, 2$, and leave the proof for the case f_1^n, f_3^n to the reader since the recurrence forms are similar. By Lemma 2.2 , for $i = 0, 2$,

$$\begin{aligned}
\widehat{f_i^n}(c^n) &= \widehat{f_0^{n-1}}(c^{n-1}) \pm 2 \cdot \widehat{f_0^{n-4}}(c^{n-4})), \\
\textit{or} \quad &= \widehat{f_0^{n-1}}(c^{n-1}) \pm 2 \cdot \widehat{f_0^{n-4}}(c^{n-4})) \pm 4 \cdot \widehat{f_1^{n-5}}(c^{n-5}), \\
\textit{or} \quad &= \widehat{f_0^{n-1}}(c^{n-1}) \pm 2 \cdot \widehat{f_0^{n-4}}(c^{n-4})) \pm 4 \cdot \widehat{f_1^{n-5}}(c^{n-5} + e_{2^{n-6}}).
\end{aligned} \tag{18}$$

We prove the inequality for the first case and the second case, while the third case is similar. If $\widehat{f_i^n}(c^n) = \widehat{f_0^{n-1}}(c^{n-1}) \pm 2 \cdot \widehat{f_0^{n-4}}(c^{n-4}))$, then by Lemma 2.3 and induction,

$$\begin{aligned}
&\left|\widehat{f_i^s}(c^s)\right| \\
&\leq \left|\widehat{f_0^{s-1}}(c^{s-1})\right| + 2\left|\widehat{f_0^{s-4}}(c^{s-4})\right| \\
&< \tfrac{1}{4} \cdot (\widehat{F_3^{s+1}}(0) + 2\widehat{F_3^{s-2}}(0)) \\
&< \tfrac{1}{4} \cdot (2\widehat{F_3^{s}}(0) + 2\widehat{F_3^{s-1}}(0)) \\
&= \tfrac{1}{4} \cdot \widehat{F_3^{s+2}}(0).
\end{aligned} \tag{19}$$

When $\widehat{f_i^n}(c^n) = \widehat{f_0^{n-1}}(c^{n-1}) \pm 2 \cdot \widehat{f_0^{n-4}}(c^{n-4})) \pm 4 \cdot \widehat{f_1^{n-5}}(c^{n-5})$, then by Lemma 2.3 and induction again,

$$\begin{aligned}
&\left|\widehat{f_i^s}(c^s)\right| \\
&< \tfrac{1}{4} \cdot (\widehat{F_3^{s+1}}(0) + 2\widehat{F_3^{s-2}}(0) + 4\widehat{F_3^{s-3}}(0)) \\
&= \tfrac{1}{4} \cdot \widehat{F_3^{s+2}}(0).
\end{aligned} \tag{20}$$

■

Theorem 2.5 *For all $c^n = (x_0, \cdots, x_{n-1}) \neq 0$ and all $n \geq 3$,*

$$\left|\widehat{F_3^n}(c^n)\right| < \widehat{F_3^n}(0).$$

Proof. For the few cases $n \leq 10$, we have the correctness by the computer's computation results. Now assume $n > 10$.

Since $c^n \neq 0$, by Lemma 1.2, $\widehat{F_3^n}(x_0, \cdots, x_{n-1}) = \widehat{F_3^n}(x_j, \cdots, x_{n-j-1})$ for all $j \in [0, n-1]$. Thus we assume $c_1 = 1$. By Lemma 2.4, we have

$$\begin{aligned}
&\left|\widehat{F_3^n}(c^n)\right| \\
&= \left|\widehat{f_0^{n-2}}(c^{n-2}) + (-1)^{c_{n-2}} \cdot \widehat{f_2^{n-2}}(c^{n-2}) + (-1)^{c_{n-1}} \cdot \widehat{f_1^{n-2}}(c^{n-2}) + (-1)^{c_{n-2}+c_{n-1}} \cdot \widehat{f_3^{n-2}}(c^{n-2})\right| \\
&\leq \left|\widehat{f_0^{n-2}}(c^{n-2})\right| + \left|\widehat{f_2^{n-2}}(c^{n-2})\right| + \left|\widehat{f_1^{n-2}}(c^{n-2})\right| + \left|\widehat{f_3^{n-2}}(c^{n-2})\right| \\
&< \tfrac{1}{4} \cdot (\widehat{F_3^n}(0) + \widehat{F_3^n}(0) + \widehat{F_3^n}(0) + \widehat{F_3^n}(0)) \\
&= \widehat{F_3^n}(0).
\end{aligned}$$

■

3 Conclusion

In this paper we prove the conjecture proposed in [1], i.e. the nonlinearity of $F_3^n(x_0, \cdots, x_{n-1})$ is the same as its weight. Recently Cusick remarked that computer's results imply that the Conjecture may be extended to RSBF with SANF $x_0 x_a x_b (b > a > 0)$ in the case of odd n. However it seems difficult to prove that. It is interesting to note that it has been proved in [7] that the nonlinearity of $F_2^n(x_0, \cdots, x_{n-1}) = \sum_{0 \leq i \leq n-1} x_i x_{i+s(mod\ n)}$ is the same as its weight if $\frac{n}{gcd(n,s)}$ is even. These properties show that rotation symmetric Boolean functions have nice cryptographic applications. Whether higher degree RSBFs have these properties is an interesting topic for further research.

References

[1] Cusick T.W. and Stănică P.: Fast evaluation,weights and nonlinearity of rotation-symmetric functions, *Discrete Mathematics*, 258(2002), 289-301.

[2] Filiol E. and Fontaine C.: Highly nonlinear balanced Boolean functions with a good correlation-immunity. In Advances in *Cryptology -EUROCRYPT'98*, Springer-Verlag, 1998.

[3] Pieprzyk J. and Qu C.X.: Fast hashing and rotation symmetric functions. *Journal of Universal Computer Science*, 5(1),1999,20-31.

[4] Mariai S., Shimoyama T. and Kaneko T.: Higher order differential attack using chosen higher order differences, in: *Selected Areas in Cryptography-SAC'98*, Lectures Notes in Computer Science. Vol. 1556, Springer, Berlin, 1999, 106-117.

[5] Stănică P. and Maitra S.: Rotation symmetric Boolean functions- Count and cryptographic properties. *Discrete Applied Mathematics*, 156,2008, 1567-1580.

[6] Kavut S., Maitra S. and Yucel M.D.: Search for Boolean functions with excellent profiles in the rotation symmetric class, *IEEE Transaction on Information Theory*, 53(5),2007, 1743-1751.

[7] Kim H., Park S. and Hahn S.G.: On the weight and nonlinearity of homogeneous rotation symmetric Boolean functions of degree 2. *Discrete Applied Mathematics*, 157,2009, 428-432.

[8] Ciungu L. C.: Cryptographic Boolean functions: Thus-Morse sequences, weight and nonlinearity. PHD thesis, the University at Buffalo, State University of New York, 2010.03.